Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of claims:

1 – 11. (cancelled)

12. (currently amended) A method for verifying a signature for a message m in a data communication system established between a sender and a recipient, said sender generating masked signature components (r, s, c), where r is an integer derived from a coordinate of a first short term public key kP, s is a signature component derived by binding a second short term private key, the message m and short and long term private keys, and c is a second signature component obtained by combining said first and second short term private keys, said method comprising the steps of a verifier:

a) obtaining a pair of signature components $(\bar{s}, r)$, said component $\bar{s}$ being derived from said first and second signature components generated by a signor;

b) recovering a coordinate pair (x_1, y_1) corresponding to said first short term public key kP using said pair $(\bar{s}, r)$ and said message m;

c) calculating a signature component r' from one of said coordinate [[pairs]] pair; and

d) verifying said signature if $r' = r$.

13. (previously presented) A method according to claim 12 further comprising the step of said verifier receiving (r, s, c) from said signor and converting (s, r, c) to obtain said pair $(\bar{s}, r)$.

14. (previously presented) A method according to claim 12 further comprising the step of said signor converting (s, r, c) to said pair $(\bar{s}, r)$ and said signor sending said pair $(\bar{s}, r)$ to said verifier.

15. (previously presented) A method according to claim 12 wherein said coordinate pair (x_1,y_1) is calculated using a pair of values u and v, said values u and v derived from said pair $(\bar{s},r)$ and said message m.

16. (previously presented) A method according to claim 15 wherein said coordinate pair (x_1,y_1) is calculated as $(x_1,y_1) = uP + vQ$, wherein P is a point on an elliptic curve E and Q is a public verification key of said signor derived from P as $Q = dP$.

17. (previously presented) A method according to claim 15 wherein said value u is computed as $u = \bar{s}^{-1}e \bmod n$ and said value v is computed as $v = \bar{s}^{-1}r \bmod n$, e being a representation of said message m.

18. (previously presented) A method according to claim 17 wherein e is calculated as $e = H(m)$, $H(\,)$ being a hash function of said signor and being known to said verifier.

19. (previously presented) A method according to claim 12 wherein said coordinate x_1 is first converted to an integer $\bar{x}_1$ prior to calculating said component r'.

20. (previously presented) A method according to claim 19 wherein said component r' is calculated as $r' = \bar{x}_1 \bmod n$.

21. (previously presented) A method according to claim 12 wherein prior to calculating said component r', said coordinate pair (x_1,y_1) is first verified, whereby if said coordinate pair (x_1,y_1) is a point at infinity, then said signature is rejected.